IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: Raymond Harper	)	Confirmation No: 2178
	)	
Serial No.: 10/729,293	)	Group Art Unit: 2132
	)	
Filed: December 5, 2003	)	Examiner: Almeida, Devin E.
	)	
For: SARTS PASSWORD MANAGER	)	Atty. Docket No.: 190250-1500

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed February 29, 2008, responding to the final Office Action mailed October 30, 2007.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 20-0778.

I. Real Party in Interest

The real party in interest is AT&T Delaware Intellectual Property Inc., formerly known as BellSouth Intellectual Property Corporation, a Corporation of the State of Delaware, having a place of business at 824 Market Street, Suite 425, Wilmington, DE 19801.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1-29 stand finally rejected. No claims have been allowed. The rejections of claims 1-29 are appealed.

IV. Status of Amendments

No amendments have been made subsequent to the final office action mailed October 30, 2007. The claims in the attached Claims Appendix (see below) reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter

described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a password management system. The system comprises graphical user interface logic (FIG. 2, 350, 360) residing on a first computer system (FIG. 1, 110) operable to receive a current password from a user, prompt the user to determine whether the user desires to change the current password, and responsive to the user response receive a new password. Applicant's specification, page 12, lines 7-12. Password confirmation logic (FIG. 2, 350) residing on the first computer system (FIG. 1, 110) is operable to confirm the current password associated with the user on a switched access remote test system (FIG. 1, 120) residing on a second computer system (FIG. 1, 115) remote from the first computer system (FIG. 1, 110). Applicant's specification, pages 12-13, lines 24-15. The system further comprises password administration logic (FIG. 2, 350) residing on the first computer system (FIG. 1, 110), responsive to the password confirmation logic (FIG. 2, 350) and the graphical user interface (FIG. 2, 350, 360), operable to receive the new password and to change the current password on the switched access remote test system (FIG. 1, 120). Applicant's specification, page 13, lines 16-19. The system also comprises expiration logic (FIG. 2, 350) residing on the first computer system (FIG. 1, 110) operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system (FIG. 1, 120) residing on the second computer system (FIG. 1, 115) and is operable to cause the user to be

prompted to change the current password if the current password is determined to be approaching its expiration. Applicant's specification, page 13, lines 16-21.

Embodiments according to independent claim 12 describe a method of managing passwords. The method comprises providing a user with a graphical user interface residing on a first computer system (FIG. 1, 110) and receiving a current password from the user via the graphical user interface for a switched access remote test system (FIG. 1, 120) residing on a second computer system (FIG. 1, 115) remote from the first computer system (FIG. 1, 110). Applicant's specification, page 12, lines 13-23. The method further comprises determining at the first computer system (FIG. 1, 110) if the current password is approaching its expiration prior to logging onto the switched access remote test system (FIG. 1, 120) residing on the second computer system (FIG. 1, 115) and prompting the user on whether to change the current password. Applicant's specification, page 12, lines 5-12 and page 13, lines 16-21. The method also comprises receiving a new password from the user responsive to the user response to the prompting; confirming the current password with the switched access remote test system (FIG. 1, 120); and requesting that the switched access remote test system (FIG. 1, 120) change the password responsive to the user response to the prompting. Applicant's specification, page 13, lines 22-23 and page 14, lines 10-13.

Embodiments according to independent claim 21 describe a computer readable medium having a program for managing passwords. Applicant's specification, pages 11-12, lines 1-2. The program is operable to perform providing a user with a graphical user interface residing on a first computer system (FIG. 1, 110) and receiving a current

password from the user via the graphical user interface for a switched access remote test system (FIG. 1, 120) residing on a second computer system (FIG. 1, 115) remote from the first computer system (FIG. 1, 110). Applicant's specification, page 12, lines 13-23. The program further performs prompting the user on whether to change the current password and determining at the first computer system (FIG. 1, 110) if the current password is approaching its expiration prior to logging onto the switched access remote test system (FIG. 1, 120) residing on the second computer system (FIG. 1, 115). Applicant's specification, page 12, lines 5-12 and page 13, lines 16-21. The program also performs receiving a new password from the user responsive to the user response to the prompting; confirming the current password with the switched access remote test system (FIG. 1, 120); and requesting that the switched access remote test system (FIG. 1, 120) change the password responsive to the user response to the prompting. Applicant's specification, page 13, lines 22-23 and page 14, lines 10-13.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-10 and 12-29 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Limsico* (U.S. Patent No. 5,793,952) in view of *Ackroff* (U.S. Patent No. 5,105,438) in further view of *Kadooka* (U.S. Patent No. 5,606,663).

Claim 11 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Limsico* in view of *Ackroff* in further view of *Kadooka* in further view of *Goldberg* (U.S. Patent No. 5,748,890).

VII. Arguments

The Appellant respectfully submits that Applicant's claims 1-29 are patentable. The Appellant respectfully requests that the Board of Patent Appeals overturn the rejection of those claims at least for the reasons discussed below.

A. The *Limsico* Disclosure

Limsico describes a password changing routine that provides a graphic user interface. In response to receiving a request from a host machine to change a password, the routine sends a user's new password as entered in a password changer window 100. *See* col. 5, lines 3-12 and col. 10, lines 7-18. *Limsico* describes that a host system tracks an expiration date for a user's password and does not disclose that the password changing routine is capable of performing this function. Rather, the password changing routine relays messages and prompts generated by the host system.

B. The *Ackroff* Disclosure

Ackroff describes an Intelligent Network Channeling Terminating Equipment device that can measure the frequency and level of signals that are sent from a remote location such as from a Switched Access Remote Test System. *See* col. 5, lines 1-6.

C. The *Kadooka* Disclosure

Kadooka describes a password updating system where a computer system which requires a password has a comparator unit 2, period setting unit 3, hysteresis memory unit 4, update processing unit 5, and input unit 6 residing with the computer system. The period setting unit 3, update processing unit 5, and input unit 6 retrieve information in or store information to the hysteresis memory unit 4 on the same computer system.

D. The *Goldberg* Disclosure

Goldberg describes a method and system for authenticating and auditing access by a user to non-natively secured applications through the use of a single password. *See* col. 2, lines 24-27.

E. Applicant's Claims 1-10

As recited in independent claim 1, Applicant claims:

> A password management system, comprising:
> graphical user interface logic residing on a first computer system operable to receive a current password from a user, prompt the user to determine whether the user desires to change the current password, and responsive to the user response receive a new password;
> password confirmation logic residing on the first computer system operable to confirm the current password associated with the user on a switched access remote test system residing on a second computer system remote from the first computer system;
> password administration logic residing on the first computer system, responsive to the password confirmation logic and the graphical user interface, operable to receive the new password and to change the current password on the switched access remote test system; and
> ***expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test***

system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration.

(Emphasis added).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that *Limsico* in view of *Ackroff* in further view of *Kadooka* does not disclose, teach, or suggest at least "expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration," as emphasized above.

For instance, *Limsico* describes a password changing routine that provides a graphic user interface. In response to receiving a request from a host machine to change a password, the routine sends a user's new password as entered in a password changer window 100. *See* col. 5, lines 3-12 and col. 10, lines 7-18. *Limsico* describes that a host system tracks an expiration date for a user's password and does not disclose that the password changing routine is capable of performing this function. Rather, the password changing routine relays messages and prompts generated by the host system.

Accordingly, *Limsico* fails to disclose that the local machine 310 has expiration logic operable to determine if a current password is approaching its expiration prior to logging onto a remote machine 320. For at least this reason, *Limsico* fails to teach or suggest at least "expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the

switched access remote test system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration," as recited in claim 1.

Further, *Ackroff* describes an Intelligent Network Channeling Terminating Equipment device that can measure the frequency and level of signals that are sent from a remote location such as from a Switched Access Remote Test System. *See* col. 5, lines 1-6. *Ackroff* individually or in combination with *Limsico* does not teach or suggest at least "expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration," as recited in claim 1.

Kadooka describes a password updating system where a computer system which requires a password has a comparator unit 2, period setting unit 3, hysteresis memory unit 4, update processing unit 5, and input unit 6 residing with the computer system. The period setting unit 3, update processing unit 5, and input unit 6 retrieve information in or store information to the hysteresis memory unit 4 on the same computer system. As such, *Kadooka* individually or in combination with *Limsico* fails to teach or suggest at least "expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration," as recited in claim 1.

Each of the aforementioned cited references fails to teach or suggest features alleged in the final Office Action. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 1. Further, Applicant submits that the claimed features would not be obvious to a person of ordinary skill in the art. As such, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Limsico* in view of *Ackroff* in further view of *Kadooka* has not been made, and the rejection of claim 1 should be overturned.

In the final Office Action, in response to prior arguments, it states that "Kadooka teaches expiration logic residing on a first computer (Limsico's local machine) system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on a second computer system (Limsico's remote machine) and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration (see figure 4a)." Page 2. However, as explained above, both *Kadooka* and *Limsico* describe that a host computer of a password protected computer system has password routines that reside on the host computer having the password protected computer system. These password routines do not reside on a second computer. Therefore, the proposed combination does not teach or suggest all of the features of claim 1.

For at least the reasons given above, claim 1 is allowable over the cited art of record. Since claims 2-10 depend from and include all of the features of claim 1 and recite additional features, claims 2-10 are allowable as a matter of law over the cited art of

record. As an example, claim 8 depends from claims 1 and 6-7 and includes a variety of features not taught or suggested by the cited art, such as "wherein the password administration logic performs a password change upon receiving a request to change the password from the graphical user interface," "wherein the password administration logic performs a password change upon receiving a confirmation of the password from the password confirmation logic," and "wherein the password administration logic is operable to send the current password and the new password to the switched access remote test system and receive a response from the switched access remote test system, and compare the response to a plurality of expected responses."

Therefore, the rejections of claims 1-10 should be overturned.

F. Applicant's Claim 11

Goldberg fails to remedy the deficiencies of *Limsico*, *Ackroff*, and *Kadooka*. Since claim 11 depends from and includes all of the features of claim 1 and recites additional features, claim 11 is allowable as a matter of law over the cited art of record. As an example, claim 11 recites "wherein the password management system is operable to interact with at least two switched access remote testing systems through a second graphical user interface that forms a wrapper for said at least two switched access remote testing systems" which is not taught or suggested by the cited art.

Therefore, the rejection of claim 11 should be overturned.

G. Applicant's Claims 12-20

As recited in independent claim 12, Applicant claims:

> A method of managing passwords, comprising:
> providing a user with a graphical user interface residing on a first computer system;
> receiving a current password from the user via the graphical user interface for a switched access remote test system residing on a second computer system remote from the first computer system;
> ***determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system***;
> prompting the user on whether to change the current password;
> receiving a new password from the user responsive to the user response to the prompting;
> confirming the current password with the switched access remote test system; and
> requesting that the switched access remote test system change the password responsive to the user response to the prompting.

(Emphasis added).

Applicant respectfully submits that independent claim 12 is allowable for at least the reason that *Limsico* in view of *Ackroff* in further view of *Kadooka* does not disclose, teach, or suggest at least "determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as emphasized above.

For example, *Limsico* describes a password changing routine that provides a graphic user interface. In response to receiving a request from a host machine to change a password, the routine sends a user's new password as entered in a password changer window 100. *See* col. 5, lines 3-12 and col. 10, lines 7-18. *Limsico* describes that a host system tracks an expiration date for a user's password and does not disclose that the password changing routine is capable of performing this function.

Rather, the password changing routine relays messages and prompts generated by the host system.

Accordingly, *Limsico* fails to disclose that the local machine 310 has expiration logic operable to determine if a current password is approaching its expiration prior to logging onto a remote machine 320. For at least this reason, *Limsico* fails to teach or suggest at least "determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as recited in claim 12.

Further, *Ackroff* describes an Intelligent Network Channeling Terminating Equipment device that can measure the frequency and level of signals that are sent from a remote location such as from a Switched Access Remote Test System. *See* col. 5, lines 1-6. *Ackroff* individually or in combination with *Limsico* does not teach or suggest at least "determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as recited in claim 12.

Kadooka describes a password updating system where a computer system which requires a password has a comparator unit 2, period setting unit 3, hysteresis memory unit 4, update processing unit 5, and input unit 6 residing with the computer system. The period setting unit 3, update processing unit 5, and input unit 6 retrieve information in or store information to the hysteresis memory unit 4 on the same computer system. As such, *Kadooka* individually or in combination with *Limsico* and *Ackroff* fails to teach or suggest at least "determining at the first computer system if the

current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as recited in claim 12.

Each of the aforementioned cited references fails to teach or suggest features alleged in the final Office Action. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 12. Further, Applicant submits that the claimed features would not be obvious to a person of ordinary skill in the art. As such, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Limsico* in view of *Ackroff* in further view of *Kadooka* has not been made, and the rejection of claim 12 should be overturned.

In the final Office Action, in response to prior arguments, it states that "Kadooka teaches expiration logic residing on a first computer (Limsico's local machine) system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on a second computer system (Limsico's remote machine) and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration (see figure 4a)." Page 3. However, as explained above, both *Kadooka* and *Limsico* describe that a host computer of a password protected computer system has password routines that reside on the host computer having the password protected computer system. These password routines do not reside on a second computer. Therefore, the proposed combination does not teach or suggest all of the features of claim 12.

Since claims 13-20 depend from claim 12 and recite additional features, claims 13-20 are allowable as a matter of law over the cited art of record. As an example, claim 17 which depends from claim 16 and claim 12 recites "wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises receiving a response from the switched access remote test system after sending the new password" which is not taught or suggested by the cited art.

Accordingly, the rejections of claims 12-20 should be overturned.

H. Applicant's Claims 21-29

As recited in independent claim 21, Applicant claims:

> A computer readable medium having a program for managing passwords, the program operable to perform:
> providing a user with a graphical user interface residing on a first computer system;
> receiving a current password from the user via the graphical user interface for a switched access remote test system residing on a second computer system remote from the first computer system;
> prompting the user on whether to change the current password;
> ***determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system;***
> prompting the user on whether to change the current password;
> receiving a new password from the user responsive to the user response to the prompting; confirming the current password with the switched access remote test system;
> requesting that the switched access remote test system change the password responsive to the user response to the prompting.

(Emphasis added).

Applicant respectfully submits that independent claim 21 is allowable for at least the reason that *Limsico* in view of *Ackroff* in further view of *Kadooka* does not disclose,

teach, or suggest at least "determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as emphasized above.

For instance, *Limsico* describes a password changing routine that provides a graphic user interface. In response to receiving a request from a host machine to change a password, the routine sends a user's new password as entered in a password changer window 100. *See* col. 5, lines 3-12 and col. 10, lines 7-18. *Limsico* describes that a host system tracks an expiration date for a user's password and does not disclose that the password changing routine is capable of performing this function. Rather, the password changing routine relays messages and prompts generated by the host system.

Accordingly, *Limsico* fails to disclose that the local machine 310 has expiration logic operable to determine if a current password is approaching its expiration prior to logging onto a remote machine 320. For at least this reason, *Limsico* fails to teach or suggest at least "determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as recited in claim 21.

Further, *Ackroff* describes an Intelligent Network Channeling Terminating Equipment device that can measure the frequency and level of signals that are sent from a remote location such as from a Switched Access Remote Test System. *See* col. 5, lines 1-6. *Ackroff* individually or in combination with *Limsico* does not teach or suggest at least "determining at the first computer system if the current password is approaching its

expiration prior to logging onto the switched access remote test system residing on the second computer system," as recited in claim 21.

Kadooka describes a password updating system where a computer system which requires a password has a comparator unit 2, period setting unit 3, hysteresis memory unit 4, update processing unit 5, and input unit 6 residing with the computer system. The period setting unit 3, update processing unit 5, and input unit 6 retrieve information in or store information to the hysteresis memory unit 4 on the same computer system. As such, *Kadooka* individually or in combination with *Limsico* and *Ackroff* fails to teach or suggest at least "determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system," as recited in claim 21.

Each of the aforementioned cited references fail to teach or suggest features alleged in the final Office Action. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 21. Further, Applicant submits that the claimed features would not be obvious to a person of ordinary skill in the art. As such, a *prima facie* case establishing an obviousness rejection by the proposed combination of *Limsico* in view of *Ackroff* in further view of *Kadooka* has not been made, and the rejection of claim 21 should be overturned.

In the final Office Action, in response to prior arguments, it states that "Kadooka teaches expiration logic residing on a first computer (Limsico's local machine) system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on a second computer

system (Limsico's remote machine) and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration (see figure 4a)." Page 3. However, as explained above, both *Kadooka* and *Limsico* describe that a host computer of a password protected computer system has password routines that reside on the host computer having the password computer system. These password routines do not reside on a second computer. Therefore, the proposed combination does not teach or suggest all of the features of claim 21.

Since claims 22-29 depend from claim 21 and recite additional features, claims 22-29 are allowable as a matter of law over the cited art of record. As an example, claim 28 depends from claims 21 and 25-27 and includes a variety of features not taught or suggested by the cited art, such as "wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises sending the new password to the switched access remote test system along with the current password," "wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises receiving a response from the switched access remote test system after sending the new password," "comparing the received response with a plurality of expected responses," and "providing an error message to the user responsive to the comparing the received response."

Accordingly, the rejections of claims 21-29 should be overturned.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be overturned. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: _____/CWG/_____
Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A password management system, comprising:

graphical user interface logic residing on a first computer system operable to receive a current password from a user, prompt the user to determine whether the user desires to change the current password, and responsive to the user response receive a new password;

password confirmation logic residing on the first computer system operable to confirm the current password associated with the user on a switched access remote test system residing on a second computer system remote from the first computer system;

password administration logic residing on the first computer system, responsive to the password confirmation logic and the graphical user interface, operable to receive the new password and to change the current password on the switched access remote test system; and

expiration logic residing on the first computer system operable to determine if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system and is operable to cause the user to be prompted to change the current password if the current password is determined to be approaching its expiration.

2. The system of claim 1, wherein the password confirmation logic is operable to send the current password to the switched access remote test system and receive a response from the switched access remote test system.

3. The system of claim 2, wherein the password confirmation logic is operable to compare the response with a plurality of expected responses and determine whether the current password provided by the user is valid.

4. The system of claim 3, wherein the response is an alphanumeric string, and the plurality of expected responses comprises erroneous responses and successful responses.

5. The system of claim 4, wherein the password confirmation logic is operable to instruct the graphical user interface logic to provide any of a plurality of error messages to the user upon the password confirmation logic determining that the current password provided by the user is not valid.

6. The system of claim 1, wherein the password administration logic performs a password change upon receiving a request to change the password from the graphical user interface.

7. The system of claim 6, wherein the password administration logic performs a password change upon receiving a confirmation of the password from the password confirmation logic.

8. The system of claim 7, wherein the password administration logic is operable to send the current password and the new password to the switched access remote test system and receive a response from the switched access remote test system, and compare the response to a plurality of expected responses.

9. The system of claim 6, wherein the password administration logic is operable to instruct the graphical user interface logic to provide any of a plurality of error messages to the user upon the password administration logic determining that the new password provided by the user was not accepted by the switched access remote test system.

10. The system of claim 1, further comprising:

a password file operable to store a set of data comprising the expiration date of the current password, wherein the expiration logic is operable to read the password file and request that the graphical user interface notify the user that the current password is nearing expiration responsive to the expiration date.

11. The system of claim 1, wherein the password management system is operable to interact with at least two switched access remote testing systems through a second graphical user interface that forms a wrapper for said at least two switched access remote testing systems.

12. A method of managing passwords, comprising:

providing a user with a graphical user interface residing on a first computer system;

receiving a current password from the user via the graphical user interface for a switched access remote test system residing on a second computer system remote from the first computer system;

determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system;

prompting the user on whether to change the current password;

receiving a new password from the user responsive to the user response to the prompting;

confirming the current password with the switched access remote test system; and

requesting that the switched access remote test system change the password responsive to the user response to the prompting.

13. The method of claim 12, wherein the confirming the current password further comprises:

sending the current password to the switched access remote test system; and

receiving a response from the switched access remote test system.

14. The method of claim 13, wherein the confirming the current password further comprises comparing the response from the switched access remote test system with a plurality of expected responses.

15. The method of claim 14, wherein the confirming the current password further comprises notifying the user of an error responsive to comparing the response from the switched access remote test system.

16. The method of claim 12, wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises sending the new password to the switched access remote test system along with the current password.

17. The method of claim 16, wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises receiving a response from the switched access remote test system after sending the new password.

18. The method of claim 17, further comprising comparing the received response with a plurality of expected responses.

19. The method of claim 18, further comprising providing an error message to the user responsive to the comparing the received response.

20. The method of claim 12, further comprising:

reading a password file to determine an expiration date associated with the current password; and

prompting the user to change the password responsive to determination of the expiration date.

21. A computer readable medium having a program for managing passwords, the program operable to perform:

providing a user with a graphical user interface residing on a first computer system;

receiving a current password from the user via the graphical user interface for a switched access remote test system residing on a second computer system remote from the first computer system;

prompting the user on whether to change the current password;

determining at the first computer system if the current password is approaching its expiration prior to logging onto the switched access remote test system residing on the second computer system;

receiving a new password from the user responsive to the user response to the prompting; confirming the current password with the switched access remote test system;

requesting that the switched access remote test system change the password responsive to the user response to the prompting.

22. The computer readable medium of claim 21, wherein the confirming the current password further comprises:

sending the current password to the switched access remote test system; and

receiving a response from the switched access remote test system.

23. The computer readable medium of claim 22, wherein the confirming the current password further comprises comparing the response from the switched access remote test system with a plurality of expected responses.

24. The computer readable medium of claim 23, wherein the confirming the current password further comprises notifying the user of an error responsive to the comparing the response from the switched access remote test system.

25. The computer readable medium of claim 21, wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises sending the new password to the switched access remote test system along with the current password.

26. The computer readable medium of claim 25, wherein the requesting that the switched access remote test system change the password responsive to the user response to the prompting further comprises receiving a response from the switched access remote test system after sending the new password.

27. The computer readable medium of claim 26, the program further operable to perform comparing the received response with a plurality of expected responses.

28. The computer readable medium of claim 27, the program further operable to perform providing an error message to the user responsive to the comparing the received response.

29. The computer readable medium of claim 21, the program further operable to perform:

reading a password file to determine an expiration date associated with the current password; and

prompting the user to change the password responsive to determination of the expiration date.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.